AGENCY OF HUMAN SERVICES

AHS Access Authorization and Enforcement Standard

Jack Green

10/3/2013

The purpose of this procedure is to facilitate the implementation of the Vermont Health Connector's security control requirements for the Access Authorization and Enforcement (AC-3, AC-6, AC-6(1), AC-6(2)) Controls.

Revision History

Date	Version	Description	Author
	1.0	Created Document	Department of Children and Family
8/16/2013	2.0	Document revised for VHC standards	Jack Green
10/10/2013	3.0	Procedures reviewed and adapted for VHC business processes and security requirements	Jack Green

PURPOSE/STANDARD STATEMENT:

The purpose of this procedure is to facilitate the implementation of the Vermont Health Connector's (VHC) security control requirements for the Access Authorization and Enforcement (AC-3, AC-6, AC-6(1), AC-6(2)) Controls.

The information systems covered in this procedure document contain but are not limited to the following:

- VHC website
- VHC Portal
- VHC workstations and mobile phones
- Network Accounts
- E-Mail accounts

SCOPE

The scope of this standard includes the VHC and its constituent systems only

.

STANDARD

Obtaining access authorization

1. Access control policy will be used and enforced by the Security and Privacy Manager to control access between all users of any VHC Information System. Below is the process for access authorization for all mentioned VHC Information Systems:
    - Initial access to VHC network, email, and employee workstation is provisioned upon employee onboarding process and is authorized by Human Resources Manager and employee supervisor.
    - Access to the VHC Website is overseen by the VHC Website System Administrator.
    - Access to the VHC Customer Portal for the Vermont constituents is overseen by MOAs (Marketplace Assister Organization). MOA Access is granted only when a grant has been awarded and processed.
    - Access to the VHC State Portal for the Vermont VHC workers is overseen by MOAs. MOA Access is granted only when a grant has been awarded and processed.
    - Access to the VHC State WAN for the Vermont VHC workers is overseen by MOAs. MOA Access is granted only when a grant has been awarded and processed.

- Access to the VHC Administration for the Connector Admins is overseen by PCG ITD. Access is granted once an email request is sent to PCG ITD by the LANDesk requestor.
    i. Connector Admins receive full viewing and edit rights.
    ii. System Administrators must ensure all users with privileged functions within the system (i.e. security functions, administrative functions) must use non-privileged accounts when accessing other system functions.
        1. Non-privileged accounts must be established in addition to the privileged for these users to ensure separation of duties.

2. System Administrators for the above mentioned systems will ensure that all users will have their access levels limited to only the roles and responsibilities needed to perform in the system.

Sensitive data authorization

1. System owners document and define appropriate access levels to sensitive data. All access levels given to users will then be documented by the system administrator to ensure proper logging.
2. Any sensitive data that need be shared will be required to go through a review and authorization process prior to being shared. The data or system owner must provide authorization of sharing the sensitive data.
3. All information defined as sensitive and transmitted by or through the Vermont Health Connector will be encrypted automatically.
4. Any encryption technologies used at the Connector for data or data transmissions will then go through an approval process and then be managed by the IT department or an approved provider.

Access delegation

1. In order to delegate access in any system, either verbal or written authorization must be logged and stored electronically. Any action taken on the behalf of another user must be authorized and the transactions logged by the person facilitating the delegated authority.

Access revocation

1. In order to ensure access revocation, the access levels delegated to the user of record will automatically be reset once that user has left the system. If the user requires access delegation at a later time they must receive verbal or written authorization again.

Access review

1. The system administrators must audit all roles or accounts which invoke any privileged activities.
2. The System Administrator reviews the list of users for their system quarterly and is then required to validate in all cases that the users have appropriate access and security levels.
3. Users who are identified as having unauthorized or inappropriate access must be logged and their access levels must be updated to reflect what is deemed authorized or appropriate.

IMPORTANT INFORMATION

These procedures can be found at http://dvha-intra.ahs.state.vt.us/policies-protocols/InfoSec